



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of: Shinsuke MORIAI

Group Art Unit: 2134

Serial Number: 09/931,858

Examiner: Christopher J. Brown

Filed: August 20, 2001

Confirmation Number: 3549

For: DATA TERMINAL DEVICE CAPABLE OF CONTINUING TO DOWNLOAD
ENCRYPTED CONTENT DATA AND A LICENSE OR REPRODUCE
ENCRYPTED CONTENT DATA WITH ITS CASING IN THE FORM OF A
SHELL CLOSED

Attorney Docket Number: 011049

Customer Number: 38834

SUBMISSION OF APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

November 1, 2006

Sir:

Applicant submits herewith an Appeal Brief in the above-identified U.S. patent application.

Attached please find a check in the amount of \$500.00 to cover the cost for the Appeal Brief.

If any additional fees are due in connection with this submission, please charge Deposit Account No.
50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

Thomas E. Brown

Attorney for Appellant

Registration No. 44,450

Telephone: (202) 822-1100

Facsimile: (202) 822-1111

TEB/jl



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

APPEAL BRIEF FOR THE APPELLANT

Ex parte Shinsuke MORIAI (Applicant)

DATA TERMINAL DEVICE CAPABLE OF CONTINUING TO DOWNLOAD ENCRYPTED
CONTENT DATA AND A LICENSE OR REPRODUCE ENCRYPTED CONTENT DATA
WITH ITS CASING IN THE FORM OF A SHELL CLOSED

Serial Number: 09/931,858

Filed: August 20, 2001

Appeal No.:

Group Art Unit: 2134

Examiner: Christopher J. Brown

Submitted by:
Thomas E. Brown
Registration No. 44,450
Attorney for Appellant

WESTERMAN, HATTORI,
DANIELS & ADRIAN, LLP
1250 Connecticut Avenue NW, Suite 700
Washington, D.C. 20036
Tel (202) 822-1100
Fax (202) 822-1111

November 1, 2006



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re the Application of: **Shinsuke MORIAI**

Appeal No.: Unassigned

Group Art Unit: 2134

Serial Number: : **09/931,858**

Examiner: Christopher J. Brown

Filed: **August 20, 2001**

Confirmation Number: 3549

**For: DATA TERMINAL DEVICE CAPABLE OF CONTINUING TO
DOWNLOAD ENCRYPTED CONTENT DATA AND A LICENSE OR
REPRODUCE ENCRYPTED CONTENT DATA WITH ITS CASING
IN THE FORM OF A SHELL CLOSED**

Attorney Docket Number: 011049

Customer Number: 38834

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

November 1, 2006

Sir:

Applicant appeals the May 11, 2006 Final rejection of claims 1-8.

Following the Notice of Appeal filed on September 11, 2006, the following is the Applicant's (now referred to hereinbelow as "appellant") Appeal Brief.

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the subject application, which is:

Sanyo Electric Co., Ltd., 5-5, Keihanondori 2-chome, Moriguchi-shi, Osaka, Japan by an assignment recorded in the U.S. Patent and Trademark Office on August 20, 2001, at Reel 012101, Frame 0725.

11/02/2006 SZEWDIE1 00000031 09931858

01 FC:1402

500.00 0P

II. RELATED APPEALS AND INTERFERENCES

Appellant knows of no other appeals or interference proceedings related to the present appeal.

III. STATUS OF CLAIMS

Pending claims 1-8 stand rejected. No claims have been allowed, objected to or cancelled. The claims on appeal are claims 1-8.

IV. STATUS OF AMENDMENTS

No Amendments to the claims have been filed in this application.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to a data terminal device accommodated in a casing in a form of a shell and capable of continuing to download encrypted content data, a license key and the like or reproduce encrypted content data with the casing closed.

With respect to claim 1, a data terminal device (see, *e.g.*, cellular phone 100 in Fig. 1) accommodated in a casing (see, *e.g.*, main body 3000, flap 3002 and movable joint 3004 in Fig. 2a-2c) in a form of a shell (see, *e.g.*, Figs. 2a-2c; and page 8, lines 9-16), downloading from a distribution server (see, *e.g.*, distribution server 30 in Fig. 1; and page 8, lines 6-8) encrypted content data and a license key decrypting said

encrypted content data, and reproducing said encrypted content data, (see, *e.g.*, page 7, line 9 – page 8, line 3) comprising:

- a communication unit (see, *e.g.*, antenna 1102 and transmission and reception unit 1104 in Fig. 7; and page 13, lines 29-33) externally effecting a communication;

- a data recording device (see, *e.g.*, memory card 110 in Fig. 1) recording said encrypted content data and said license key therein, and receiving authentication data and outputting said license key only when said authentication data is authenticated (see, *e.g.*, page 7, line 26 – page 8, line 3);

- an interface controlling data communication (see, *e.g.*, memory interface 1200 in Fig. 7; and page 14, lines 16-17);

- a control unit (see, *e.g.*, controller 1106 in Fig. 7);

- a detection unit (see, *e.g.*, detection unit 1117 in Fig. 7; and page 8, lines 17-21) detecting whether said casing is open/closed; and

- a power supply control unit (see, *e.g.*, power control unit 1116 in Fig. 7; and page 15, lines 13-19) controlling whether to supply various components with power,

- wherein when said detection unit detects that said casing is closed after download of said encrypted content data is started, said power supply control unit controls supplying power required for a call to complete downloading said encrypted content data (see, *e.g.*, steps S1002-S1014 in the flowchart of Fig. 13; and page 27, line 14 – page 28, line 4).

With regard to claim 3, a data terminal device (see, *e.g.*, cellular phone 100 in Fig. 1) accommodated in a casing (see, *e.g.*, main body 3000, flap 3002 and movable joint 3004 in Fig. 2a-2c) in a form of a shell (see, *e.g.*, Figs. 2a-2c; and page 8, lines 9-16), downloading from a distribution server (see, *e.g.*, distribution server 30 in Fig. 1; and page 8, lines 6-8) encrypted content data and a license key decrypting said encrypted content data, and reproducing said encrypted content data (see, *e.g.*, page 7, line 9 – page 8, line 3), comprising:

a communication unit (see, *e.g.*, antenna 1102 and transmission and reception unit 1104 in Fig. 7; and page 13, lines 29-33) externally effecting a communication;

a data recording device (see, *e.g.*, memory card 110 in Fig. 1) recording said encrypted content data and said license key therein, and receiving authentication data and outputting said license key only when said authentication data is authenticated (see, *e.g.*, page 7, line 26 – page 8, line 3);

a reproduction unit (see, *e.g.*, decryption unit 1212 and music reproduction unit 1216 in Fig. 7; and page 15, lines 3-12) reproducing said encrypted content data recorded in said data recording device;

an interface controlling data communication (see, *e.g.*, memory interface 1200 in Fig. 7; and page 14, lines 16-17);

a control unit (see, *e.g.*, controller 1106 in Fig. 7);

a detection unit (see, *e.g.*, detection unit 1117 in Fig. 7; and page 8, lines 17-21) detecting whether said casing is open/closed; and

a power supply control unit (see, *e.g.*, power control unit 1116 in Fig. 7; and page 15, lines 13-19) controlling whether to supply various components with power, wherein when said detection unit detects that said casing is closed after reproduction of said encrypted content data is started, said power supply control unit controls supplying power required for a reproduction process to complete reproducing said encrypted content data (see, *e.g.*, steps S1100-S1116 in the flowchart of Fig. 14; and page 28, line 16 - page 29, line 6) .

With respect to claim 5, a data terminal device (see, *e.g.*, cellular phone 100 in Fig. 1) accommodated in a casing (see, *e.g.*, main body 3000, flap 3002 and movable joint 3004 in Fig. 2a-2c) in a form of a shell (see, *e.g.*, Figs. 2a-2c; and page 8, lines 9-16), downloading from a distribution server (see, *e.g.*, distribution server 30 in Fig. 1; and page 8, lines 6-8) encrypted content data and a license key decrypting said encrypted content data, recording said encrypted content data and said license key in a data recording device (see, *e.g.*, memory card 110 in Fig. 1; and page 7, line 9 – page 8, line 3), and reproducing said encrypted content data via said data recording device (see, *e.g.*, page 8, lines 1-3), comprising:

a communication unit (see, *e.g.*, antenna 1102 and transmission and reception unit 1104 in Fig. 7; and page 13, lines 29-33) externally effecting a communication;

an interface controlling data communication (see, *e.g.*, memory interface 1200 in Fig. 7; and page 14, lines 16-17);

a control unit (see, *e.g.*, controller 1106 in Fig. 7);

a detection unit (see, *e.g.*, detection unit 1117 in Fig. 7; and page 8, lines 17-21) detecting whether said casing is open/closed; and

a power supply control unit (see, *e.g.*, power control unit 1116 in Fig. 7; and page 15, lines 13-19) controlling whether to supply various components with power,

wherein when said detection unit detects that said casing is closed after download of said encrypted content data is started, said power supply control unit controls supplying power required for a call to complete downloading said encrypted content data (see, *e.g.*, steps S1002-S1014 in the flowchart of Fig. 13; and page 27, line 14 – page 28, line 4).

With regard to claim 7, a data terminal device (see, *e.g.*, cellular phone 100 in Fig. 1) accommodated in a casing (see, *e.g.*, main body 3000, flap 3002 and movable joint 3004 in Fig. 2a-2c) in a form of a shell (see, *e.g.*, Figs. 2a-2c; and page 8, lines 9-16), downloading from a distribution server (see, *e.g.*, distribution server 30 in Fig. 1; and page 8, lines 6-8) encrypted content data and a license key decrypting said encrypted content data, recording said encrypted content data and said license key in a data recording device (see, *e.g.*, memory card 110 in Fig. 1; and page 7, line 9 – page 8, line 3), and reproducing said encrypted content data via said data recording device (see, *e.g.*, page 8, lines 1-3), comprising:

a communication unit (see, *e.g.*, antenna 1102 and transmission and reception unit 1104 in Fig. 7; and page 13, lines 29-33) externally effecting a communication;

an interface controlling data communication (see, *e.g.*, memory interface 1200 in Fig. 7; and page 14, lines 16-17);

a control unit (see, *e.g.*, controller 1106 in Fig. 7);

a reproduction unit (see, *e.g.*, decryption unit 1212 and music reproduction unit 1216 in Fig. 7; and page 15, lines 3-12) reproducing said encrypted content data recorded in said data recording device;

a detection unit (see, *e.g.*, detection unit 1117 in Fig. 7; and page 8, lines 17-21) detecting whether said casing is open/closed; and

a power supply control unit (see, *e.g.*, power control unit 1116 in Fig. 7; and page 15, lines 13-19) controlling whether to supply various components with power,

wherein when said detection unit detects that said casing is closed after reproduction of said encrypted content data is started, said power supply control unit controls supplying power required for a reproduction process to complete reproducing said encrypted content data (see, *e.g.*, steps S1100-S1116 in the flowchart of Fig. 14; and page 28, line 16 - page 29, line 6).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

- A. The rejection of claims 1, 2, 5 and 6 under 35 USC 103(a) as being unpatentable over Sachs et al (U.S. Patent No. 6,331,865) in view of Kim (U.S. Patent No. 6,044,473 and Christensen (U.S. Patent No. 5,996,078).

B. The rejection of claims 3, 4, 7 and 8 under 35 USC 103(a) as being unpatentable over Sachs et al (U.S. Patent No. 6,331,865) in view of Kim (U.S. Patent No. 6,044,473 and Christensen (U.S. Patent No. 5,996,078).

VII: ARGUMENTS

A. **Rejection of claims 1, 2, 5 and 6 under 35 USC 103(a) as being unpatentable over Sachs et al. in view of Kim and Christensen.**

Independent Claims 1 and 5:

Independent claim 1 calls for a data recording device recording said encrypted content data and said license key therein, and receiving authentication data and outputting said license key only when said authentication data is authenticated; ... wherein when said detection unit detects that said casing is closed after download of said encrypted content data is started, said power supply control unit controls supplying power required for a call to complete downloading said encrypted content data. Independent claim 5 is drawn to a similar embodiment.

For example, as shown in the flow chart of Fig. 13 and as discussed on pages 27 and 28 of the present application, the controller 1106 determines in step S1008 whether the downloading has completed. If the controller determines that the downloading still continues, a detection unit 1117 determines whether the casing of cellular phone 100 has been closed, step S1010. If the casing is closed, the cellular phone is conferred a

status on to continue a download process until the current downloading completes, step S1012. With this status, power supply control unit 1116 continues to supply each circuit with a power supply voltage required for the call. Then the amount of data distributed or the like is monitored by controller 1106 to determine whether the downloading has completed, step S1014.

With regard to the primary reference of Sachs, the Examiner acknowledges, in line 2 of page 4 of the Action, that “Sachs does not teach power supply methods.”

Further, with regard to the secondary reference of Kim, the Examiner asserts that “Kim teaches a terminal with a switch to change the power status when the casing of the terminal is closed, (Col 3 lines 1-16).”¹

However, according to Kim:

While the display 10 turns from point A to point B, the lever 12 and the contact 13 connect when the display 10 and the main housing 20 are at an angle of less than 90 degree. At this point, the switch 11 is turned on and a signal from the switch 11 changes the power of a computer system to a power controlling mode.²

Kim indicates a system allowing display 10 to be rotated by a user to switch a current mode to a low power consumption mode. This mode prevents the user from operating a computer. Apart from this mode, there exists a power save mode (or resume

¹ Please see, lines 3-4, page 4 of the Action.

² Please see, lines 28-33, col. 3 of Kim.

mode or sleep mode) allowing the user to operate the computer (see Kim, column 2, line 66 to column 3, line 16). For example the power save mode is entered when a keyboard, a mouse and the like are not, operated for a predetermined period of time. This is done automatically by the computer regardless of the user's intention.

More importantly, it is respectfully submitted that Kim teaches that the portable computer goes into low power consumption mode when the switch 11 is actuated by the closing of the display, which is complete contrast to the present invention, for example, wherein if the casing is closed, the cellular phone is conferred a status on to continue a download process until the current downloading completes, step S1012; with this status, power supply control unit 1116 continues to supply each circuit with a power supply voltage required for the call.

In addition, it is respectfully submitted that the Examiner is clearly mis-characterizing the teachings of Christensen, since this reference does not disclose that when the power switch is turned off power is still supplied to complete the downloading of data.

Christensen et al. indicates a power management system for a computer. This system is affected without user intervention and automatically controlled by BIOS (see Christensen et al., column 1, lines 43-55).

In this regard Christensen et al. indicate that for example in a serial download operation the BIOS's timer is prevented from counting down to switch the current mode to the power management mode. The power management mode is a mode entered for example when a keyboard, a mouse and the like are not operated for a predetermined period of time, and preventing a current mode from automatically being switched to the power management mode during the serial download operation is contemplated. That is, as shown in the flowcharts of Figs. 1a and 1b, during an application processing a determination is made as to whether to reset the power management timers (S105) in the BIOS. If yes, then the application program sets the AX register equal to 6 (S107) and calls software interrupt 14h (in S109). The BIOS software interrupt routine 14h checks whether the AX register equals 6 (S112), and if so resets the power management timers (in S114). As such, the condition of the power management timers counting down during the processing of an application program is avoided by setting the AX register to 6 and calling the software interrupt 14h.

In other words, Christensen et al.'s power management mode is the same mode as Kim's power save mode (or resume mode or sleep mode) and is automatically affected by a computer regardless of the user's intention.

In contrast, claim 1 recites an invention of a data terminal device in the form of a shell, wherein when a detection unit detects that the casing in the form of the shell is closed after download of encrypted content data is started, a power supply control unit

controls supplying power required for a call to complete downloading the encrypted content data.

In other words, claim 1 recites an invention characterized in that if a user closes the casing in the form of the shell to enter a low power consumption mode preventing the user from operating the device, similarly as described in Kim, the device can nonetheless be supplied with power required until it completes downloading data.

Kim only indicates a system allowing display 10 to be rotated to change a current mode to a low power consumption mode preventing a computer from being operated. The reference neither discloses nor suggests that when the detection unit detects that the casing in the form of the shell is closed after download of encrypted content data is started, the power supply control unit supplies power required for a call to complete downloading the encrypted content data, as characterized in claim 1.

Furthermore, Christensen et al. only indicate a system preventing automatically entering a power save mode during a serial download operation. The reference neither discloses nor suggests that if a low power consumption mode preventing a user from operating a device is entered in a download operation the power supply control unit supplies power required for a call to complete the download, as required by claim 1.

In view of the above, it is respectfully submitted that the additional secondary references of Kim and Christensen each fails to teach the above-noted drawbacks and deficiencies of Sachs.

As such, it is believed that Sachs, Kim and Christensen neither disclose nor suggest a data recording device recording said encrypted content data and said license key therein, and receiving authentication data and outputting said license key only when said authentication data is authenticated; ... wherein when said detection unit detects that said casing is closed after download of said encrypted content data is started, said power supply control unit controls supplying power required for a call to complete downloading said encrypted content data, as required by claim 1.

Moreover, even if, assuming arguendo, that the Examiner's assertion, on page 2, regarding Kim teaching that when the casing is closed, Kim still teaches that a power controlling mode would be entered or continued, it is respectfully submitted that the Examiner has failed to appreciate that that in Kim when the display 10 turns from point A to point B, the switch 11 is turned on and the power of the computer is changed to a power-saving mode, which is exactly what Christensen is trying to avoid.

More specifically, Christensen discloses in col. 3, lines 6-9 that "[t]he communications program would utilize software interrupts in BIOS to prevent unwanted power management invocations during a long upload or download via the

modem.” That is, Christensen is concerned with avoiding the timers of the BIOS from counting down to a power shut down condition during, for instance, a serial download operation.

It is respectfully submitted that one of ordinary skill would not have been motivated to combine the power saving feature of Kim with the disclosure of Christensen, since the crux of Christensen’s invention is to prevent unwanted power management invocations during a long upload or download via the modem.

Accordingly, it is respectfully submitted that the Examiner’s combination rejection is improper since Christensen explicitly teaches away from the features disclosed by Kim.

Section 2143 of the MPEP has specifically stated that:

“To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference must teach or suggest all the claimed limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant’s disclosure. *In re Vaeck*, 947 F.2d 466, 20 USPQ2d 1438 (Fed. Cir. 1991).”

For at least these reasons, it is submitted that the Examiner has failed to establish a *prima facie* case of obviousness and therefore the obviousness rejection of claims 1, 2, 5 and 6 should be withdrawn.

B. Rejection of claims 3, 4, 7 and 8 under 35 USC 103(a) as being unpatentable over Sachs et al. in view of Kim and Christensen.

Independent Claims 3 and 7:

Independent claim 3 calls for a reproduction unit reproducing said encrypted content data recorded in said data recording device; ... wherein when said detection unit detects that said casing is closed after reproduction of said encrypted content data is started, said power supply control unit controls supplying power required for a reproduction process to complete reproducing said encrypted content data.

Independent claim 7 is drawn to a similar embodiment.

For example, as shown in the flow chart of Fig. 14 and as discussed on pages 28 and 29 of the present application, the controller 1106 determines in step S1108 whether the reproduction has completed. If the controller determines that the reproduction still continues, a detection unit 1117 determines whether the casing of cellular phone 100 has been closed, step S1110. If the casing is closed, the cellular phone is conferred a status on to continue a reproduction process until the content data is completely reproduced, step S1012. With this status, power supply control unit 1116 continues to

supply each circuit with a power supply voltage required for the reproduction process. Then the controller 1106 determines the reproduction has completed, step S1114.

For at least the reasons set forth above with regard to independent claims 1 and 5, it is believed that Sachs, Kim and Christensen, singly or in combination, neither disclose nor suggest a reproduction unit reproducing said encrypted content data recorded in said data recording device; ... wherein when said detection unit detects that said casing is closed after reproduction of said encrypted content data is started, said power supply control unit controls supplying power required for a reproduction process to complete reproducing said encrypted content data, as required by claim 3.

Moreover, it is submitted that the Examiner has failed to even assert that either Kim or Christensen teaches power supply control for allowing a **reproduction process** of encrypted content data to be completed when the casing of the data terminal device is closed after **reproduction** of the encrypted content data is started.

Instead, while the Examiner argues that “Christensen teaches that power management is prevented in the case of a current download over a modem,”³ the Examiner fails to appreciate that independent claims 3 and 7 concern power supply control for the **reproduction** of encrypted content data.

³ Please see, page 4, lines 9-10 of the Final Action dated May 11, 2006.

For at least these reasons, it is submitted that the Examiner has failed to establish a *prima facie* case of obviousness and therefore the obviousness rejection of claims 3, 4, 7 and 8 should be withdrawn.

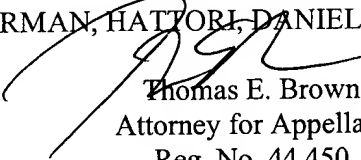
VIII. CONCLUSION

For the above reasons, Appellant requests that the Board of Patent Appeals and Interferences reverse the Examiner's rejections of claims 1-8.

In the event this paper is not timely filed, appellants hereby petition for an appropriate extension of time. The fee for any such extension may be charged to our Deposit Account No. 50-2866, along with any other additional fees which may be required with respect to this paper.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP


Thomas E. Brown
Attorney for Appellant
Reg. No. 44,450

TEB/jl

Enclosures: Claims appendix
Evidence appendix
Related proceedings appendix

CLAIMS APPENDIX

Claim 1 (Original): A data terminal device accommodated in a casing in a form of a shell, downloading from a distribution server encrypted content data and a license key decrypting said encrypted content data, and reproducing said encrypted content data, comprising:

a communication unit externally effecting a communication;

a data recording device recording said encrypted content data and said license key therein, and receiving authentication data and outputting said license key only when said authentication data is authenticated;

an interface controlling data communication;

a control unit;

a detection unit detecting whether said casing is open/closed; and

a power supply control unit controlling whether to supply various components with power,

wherein when said detection unit detects that said casing is closed after download of said encrypted content data is started, said power supply control unit controls supplying power required for a call to complete downloading said encrypted content data.

Claim 2 (Original): The data terminal device of claim 1, wherein when the data terminal device with said casing closed completes downloading said encrypted content data, said power supply control unit for example stops supplying said power and

controls a standby mode function of said various components internal to the data terminal device to shift the data terminal device to a low power consumption mode.

Claim 3 (Original): A data terminal device accommodated in a casing in a form of a shell, downloading from a distribution server encrypted content data and a license key decrypting said encrypted content data, and reproducing said encrypted content data, comprising:

- a communication unit externally effecting a communication;

- a data recording device recording said encrypted content data and said license key therein, and receiving authentication data and outputting said license key only when said authentication data is authenticated;

- a reproduction unit reproducing said encrypted content data recorded in said data recording device;

- an interface controlling data communication;

- a control unit;

- a detection unit detecting whether said casing is open/closed; and

- a power supply control unit controlling whether to supply various components with power,

wherein when said detection unit detects that said casing is closed after reproduction of said encrypted content data is started, said power supply control unit controls supplying power required for a reproduction process to complete reproducing said encrypted content data.

Claim 4 (Original): The data terminal device of claim 3, wherein when the data terminal device with said casing closed completes reproducing said encrypted content data, said power supply control unit for example stops supplying said power and controls a standby mode function of said various components internal to the data terminal device to shift the data terminal device to a low power consumption mode.

Claim 5 (Original): A data terminal device accommodated in a casing in a form of a shell, downloading from a distribution server encrypted content data and a license key decrypting said encrypted content data, recording said encrypted content data and said license key in a data recording device, and reproducing said encrypted content data via said data recording device, comprising:

- a communication unit externally effecting a communication;
- an interface controlling data communication;
- a control unit;
- a detection unit detecting whether said casing is open/closed; and
- a power supply control unit controlling whether to supply various components with power,

wherein when said detection unit detects that said casing is closed after download of said encrypted content data is started, said power supply control unit controls supplying power required for a call to complete downloading said encrypted content data.

Claim 6 (Original): The data terminal device of claim 5, wherein when the data terminal device with said casing closed completes downloading said encrypted content data, said power supply control unit for example stops supplying said power and controls a standby mode function of said various components internal to the data terminal device to shift the data terminal device to a low power consumption mode.

Claim 7 (Original): A data terminal device accommodated in a casing in a form of a shell, downloading from a distribution server encrypted content data and a license key decrypting said encrypted content data, recording said encrypted content data and said license key in a data recording device, and reproducing said encrypted content data via said data recording device, comprising:

- a communication unit externally effecting a communication;
 - an interface controlling data communication;
 - a control unit;
 - a reproduction unit reproducing said encrypted content data recorded in said data recording device;
 - a detection unit detecting whether said casing is open/closed; and
 - a power supply control unit controlling whether to supply various components with power,
- wherein when said detection unit detects that said casing is closed after reproduction of said encrypted content data is started, said power supply control unit

controls supplying power required for a reproduction process to complete reproducing said encrypted content data.

Claim 8 (Original): The data terminal device of claim 7, wherein when the data terminal device with said casing closed completes reproducing said encrypted content data, said power supply control unit for example stops supplying said power and controls a standby mode function of said various components internal to the data terminal device to shift the data terminal device to a low power consumption mode.

EVIDENCE APPENDIX

No evidence under 37 C.F.R. § 41.37(c)(1)(ix) is submitted.

RELATED PROCEEDING APPENDIX

No decisions under 37 C.F.R. § 41.37(c)(1)(x) are rendered.